CHAPTER 1

INTRODUCTION TO THE INFORMATION SECURITY PROGRAM

1-1 PURPOSE, APPLICABILITY, AND SCOPE

1. **Purpose**

a. This regulation establishes the Department of the Navy (DON) Information Security Program (ISP). The ISP applies uniform, consistent, and cost-effective policies and procedures to the classification, safeguarding, transmission and destruction of classified information. This regulation also provides guidance on security education and the industrial security program. The term "classified information" is used throughout this regulation to include classified material (i.e., any matter, document, product, or substance on or in which classified information is recorded or embodied).

b. It implements the ISP within the DON in compliance with references (a) through (e), and also implements specific requirements of references (f) through (h).

2. **Applicability.** This regulation applies to all personnel, military and civilian, assigned to or employed by any element of the DON. Personnel are individually responsible for compliance. This regulation establishes the minimum standards for classification, safeguarding, transmission and destruction of classified information as required by higher authority.

3. **Scope.** This regulation applies to all official information that has been determined under reference (a) or any predecessor Order to require protection against unauthorized disclosure and is so designated by an appropriate classifying authority. This regulation incorporates the policies of documents referenced in paragraph 1-1.1b and refers to other directives listed at the end of each chapter that relate to the protection of classified information. Each chapter also lists related documents governing other classified programs, controlled unclassified information, and the National Industrial Security Program (NISP).

4. **Special Types of Classified Information.** Certain information is governed by other regulations (see **appendix A** for definitions):

a. **Communications Security (COMSEC) Information.** COMSEC information is governed by references (i) and (ab).

b. **Sensitive Compartmented Information (SCI).** SCI is governed by reference (j) and other national, Department of Defense (DoD), and DON issuances.

c. **Special Access Programs (SAPs).** All SAPs must be authorized by the Secretary of Defense (SECDEF) or the Deputy SECDEF and are governed by references (l) through (o). The Director, Special Programs Division (N89) receives and reviews requests for SAPs and the Under Secretary of the Navy must formally approve the establishment of each SAP in coordination with the Deputy SECDEF.

d. **Single Integrated Operational Plan (SIOP) and Single Integrated Operational Plan-Extremely Sensitive Information (SIOP-ESI).** SIOP and SIOP-ESI is governed by reference (p), which is issued by the CNO (N514).

e. **Naval Nuclear Propulsion Information (NNPI).** NNPI is governed by reference (q). Certain NNPI may be unclassified but is marked with special handling instructions per reference (q).

f. **Restricted Data (RD) and Formerly Restricted Data (FRD).** RD and FRD is governed by reference (r) and the Department of Energy (DOE) Regulations issued by reference (h). **Critical Nuclear Weapons Design Information (CNWDI)** is a special category of RD whose access is governed by reference (s).

g. **Foreign Government Information (FGI).** FGI is information received from one or more foreign governments or international organizations as classified, or expected to be held in confidence. It is classified, safeguarded, and declassified as agreed between the United States (U.S.) and the foreign entity.

h. **North Atlantic Treaty Organization (NATO) Information.** NATO classified and unclassified information is governed by reference (t), which is issued by reference (u).

5. **NISP.** The NISP was established by reference (f) to safeguard classified information released to industry in a manner that is equivalent to its protection within the executive branch. It is the single, integrated, cohesive industrial security program of the U.S. to protect classified information in the possession of the contractors of all executive branch departments and agencies. The NISP applies to information classified under references (a) and (r).

6. **Controlled Unclassified Information.** Controlled unclassified information is defined and governed by laws, international agreements, E.O.s, and regulations that address the identification, marking, protection, handling, transmission, transportation, and destruction of controlled unclassified information. This regulation refers to the appropriate governing authority for these categories of controlled unclassified information:

a. For Official Use Only (FOUO) information under the Freedom of Information Act (FOIA);

b. Department of State (DOS) Sensitive But Unclassified (SBU) (formerly Limited Official Use (LOU)) information;

c. DoD and DOE Unclassified Controlled Nuclear Information (UCNI);

d. Drug Enforcement Administration (DEA) Sensitive Information;

e. Sensitive Information as defined by the Computer Security Act of 1987;

f. Unclassified information in technical documents requiring distribution statements and unclassified NNPI.

1-2 POLICY GUIDANCE

1. **Assistance Via the Chain of Command.** DON personnel are encouraged to obtain guidance or interpretation of policy and procedures in this regulation via the chain of command. Telephone inquiries may be made to the CNO (N09N2) **Security Action Hotline** at (202) 433-8856. See the CNO (N09N2) Homepage at **www.navysecurity.navy.mil**. After hours calls are recorded and returned as soon as possible.

2. **Combat Operations.** Commanding officers may modify the safeguarding requirements of this regulation as necessary to meet local conditions during combat or combat-related operations. Even under these circumstances, the provisions of this regulation shall be followed as closely as possible. This exception does not apply to regularly scheduled training exercises or operations.

3. **Waivers and Exceptions.** When conditions exist that prevent compliance with a specific safeguarding standard or costs of

compliance exceed available resources, a command may submit a request for a waiver or exception to the requirements of this regulation, in writing, via the chain of command to the CNO (N09N2). Each request shall include a complete description of the problem and describe the compensatory procedures, as appropriate. The initiating command shall assign a number using the command's Unit Identification Code (UIC) preceded by N for Navy or M for Marine Corps, W(I) for waiver or E(I) for exception, number, and year (e.g., N12345-E(I)-01-98) to each waiver or exception request. Include a point of contact and telephone number with your request. Waivers and exceptions are self-cancelling at the end of the approved time, unless a renewal request is approved by the CNO (N09N2).

a. **Waiver.** A waiver may be granted to provide temporary relief from a specific requirement pending completion of action which will result in compliance with this regulation.

b. **Exception.** An exception may be granted to accommodate a long-term or permanent inability to meet a specific requirement.

4. **Alternative or Compensatory Security Control Measures.** References (c) and (e) authorize the DON to employ alternative or compensatory security controls for safeguarding classified information. Procedures for submitting requests and requirements for approval are stated in chapter 7, paragraph 7-8.

1-3 NATIONAL AUTHORITIES FOR SECURITY MATTERS

1. **The President** of the U.S. bears executive responsibility for the security of the Nation which includes the authority to classify information for the protection of the national defense and foreign relations of the U.S. The President established standards for the classification, safeguarding, downgrading, and declassification of classified national security information (NSI) in reference (a).

2. **The National Security Council (NSC)** provides overall policy guidance on information and personnel security.

3. **The Director of the Information Security Oversight Office (ISOO)**, under the authority of the Archivist of the U.S., acting in consultation with the NSC, issues directives as necessary to implement reference (a). The directives establish national

standards for the classification and marking of classified national security information, security education and training programs, self-inspection programs, and declassification. The ISOO has the responsibility to oversee agency implementation and compliance with these directives. In this role, the ISOO conducts oversight visits at selected locations. Visits to or requests for information regarding DON commands are coordinated through the CNO (N09N2).

4. **The Security Policy Board (SPB)** is an interagency organization co-chaired by the Deputy SECDEF and the Director of Central Intelligence (DCI) created by the President to consider, coordinate, and recommend for implementation to the President, through the NSC, uniform standards, policies and procedures governing classified information and personnel security, to be implemented and applicable throughout the Federal Government.

5. **The DCI**, as the chairman of the National Foreign Intelligence Board (NFIB), issues instructions in the form of DCI directives or policy statements affecting intelligence policies and activities. The DCI is charged by reference (v) with protecting intelligence sources and methods.

6. **The Federal Bureau of Investigation (FBI)** is the primary internal security agency of the U.S. Government. It has jurisdiction over investigative matters which include espionage, sabotage, treason, and other subversive activities. The Director, Naval Criminal Investigative Service (DIRNCIS) is the investigative component of the DON and is the sole liaison with the FBI on internal security matters.

1-4 DoD SECURITY PROGRAM MANAGEMENT

1. **The Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (OASD(C^3I))** is the DoD senior official charged by the SECDEF with responsibility for developing policies and procedures governing information and personnel security, including atomic energy policy programs. The Deputy Assistant Secretary of Defense (Security and Information Operations (S&IO)) produces references (e) and (w). Reference (e) is the primary source for the policies and procedures in this regulation.

2. **The Under Secretary of Defense for Policy (USD(P))** is designated as the senior official responsible for administering that portion of the DoD ISP pertaining to SAPs, the National Disclosure Policy (NDP), FGI (including NATO), and security arrangements for international programs.

3. **The Deputy Under Secretary of Defense for Policy Support (DUSD(PS))** administers international security policy and performs administrative support to the SECDEF who is designated the U.S. Security Authority for NATO (USSAN). The USSAN implements security directives issued by NATO and oversees the Central U.S. Registry (CUSR), with Army as executive agency.

4. **The National Security Agency (NSA)** provides centralized coordination and direction for signals intelligence and communications security for the U.S. Government. The DON contributes to these efforts primarily through the Commander, Naval Security Group Command (COMNAVSECGRU). The Director, NSA is authorized by the SECDEF to prescribe procedures or requirements, in addition to those in DoD regulations, for SCI and COMSEC. The authority to lower any COMSEC security standards within the DoD rests with the SECDEF.

5. **The Defense Intelligence Agency (DIA)** coordinates the intelligence efforts of the Departments of the Army, Navy, and Air Force and is responsible for development of standards, implementation, and operational management of the SCI compartments for the DoD. The Director is the Senior Official of the Intelligence Community (SOIC) of the DoD and is a member of the NFIB.

1-5 DON SECURITY PROGRAM MANAGEMENT

1. **The Secretary of the Navy (SECNAV).** The SECNAV is responsible for implementing an ISP per the provisions of E.O.s, public laws, and directives issued by the NSC, DOE, DoD, DCI, and other agencies regarding the protection of classified information.

2. **The Special Assistant for Naval Investigative Matters and Security, Office of the Chief of Naval Operations (CNO (N09N)/ DIRNCIS).** The SECNAV has designated the CNO (N09N)/DIRNCIS as the DON senior agency official under reference (a) and the DON RD management official under reference (h). The Assistant for Information and Personnel Security (CNO (N09N2))/Deputy Assistant

Director, Information and Personnel Security Programs (NCIS-21) provides staff support for these functions and responsibilities.

a. The CNO (N09N) is responsible to the SECNAV for establishing, directing, and overseeing an effective DON ISP, and for implementing and complying with all directives issued by higher authority. This responsibility includes:

(1) Formulating policies and procedures, issuing directives, and monitoring, inspecting, and reporting on the status of administration of the ISP in the DON.

(2) Implementing an industrial security program within the DON.

(3) Ensuring that persons with access to RD (including CNWDI) and FRD information are trained on appropriate classification, handling, and declassification procedures; serving as the primary point of contact for coordination with the DOE Director of Declassification on RD and FRD classification and declassification issues.

(4) Serving as primary ISP liaison with the ISOO, SPB, Office of the SECDEF and other DoD components and Federal agencies.

b. The CNO (N09N) is also responsible for establishing, administering, and overseeing the DON Personnel Security Program (PSP), and issues personnel security policy and procedures in reference (x), and publishes the Information and Personnel Security Newsletter on a quarterly basis. This newsletter is not a directive, but states the DON interpretation of security policies and procedures and provides advance notification of changes in the program. A roster of personnel assigned to the CNO (N09N2), showing each area of responsibility, is published periodically. Telephonic requests for information may be directed to the specialist having responsibility for the area of concern.

c. The DIRNCIS is responsible for investigative, law enforcement, physical security technical surveillance countermeasures, and counterintelligence (CI) policy and programs within the DON. DIRNCIS serves as the Assistant for Counterintelligence (N2E) to the Director of Naval Intelligence (DNI), and NCIS supports the national CI effort by collecting, analyzing, and disseminating information of internal security significance to DON commands.

3. **The Department of the Navy, Chief Information Officer (CIO), Office of the Assistant Secretary of the Navy (Research, Development, and Acquisition) (ASN(RD&A))** is responsible for DON implementation of reference (y). The DON CIO issues DON policies and guidance for the Information Systems Security (INFOSEC) program per reference (z), and is responsible for Information Management and Information Technology (IM/IT) policies, directives, instructions, and guidance, and approves strategies, architectures, standards, and plans for the Navy and Marine Corps.

4. **The Director, Navy International Programs Office (Navy IPO)** is responsible to the ASN(RD&A) for implementing policies and managing DON participation in international efforts concerning RD&A. The Director makes release determinations for disclosure of classified and controlled unclassified information to foreign governments and organizations in compliance with NDP, and manages certain personnel exchange programs with foreign governments.

5. **The Commandant of the Marine Corps (CMC)** administers the DON ISP within the Marine Corps. Designated functions are performed by specific organizations within the Headquarters, Marine Corps:

a. **CMC (Code ARS)** is responsible for implementation of CI and human intelligence programs.

b. **CMC (Code CIS)**, as Special Security Officer (SSO) for the Marine Corps, is responsible for guidance and implementation of SCI programs.

6. **The Director of Naval Intelligence (DNI) (CNO (N2))**, as the SOIC of the DON, is responsible for administering SCI programs for the DON. **The Office of Naval Intelligence (ONI)**, under the DNI (CNO (N2)), is responsible for the security management and implementation of SCI programs. **The Director, Security Directorate/SSO Navy (ONI-5)**, is responsible for guidance and instruction on matters concerning the security, control, and utilization of SCI.

7. **The Director, Space, Information Warfare, Command and Control (CNO (N6)), Head, Navy Defensive Information Warfare/Information Systems Security Branch (CNO (N643))**, in coordination with the DON CIO, is responsible for policy, implementation, and oversight of the DON INFOSEC program, and issues reference (aa).

8. **The Director, Special Programs Division (N89)** is designated as the DON SAP coordinator and is responsible for the management of the DON SAP Central Office, and to coordinate SAP approval, administration, support, review, and oversight per references (e), (k), and (l).

9. **The COMNAVSECGRU**, as the designated SSO for the NAVSECGRU, is responsible for signals intelligence activities and for administration of SCI programs within the DON cryptologic community.

10. **The Director, COMSEC Material System (DCMS)** administers the DON CMS program and acts as the central office of records for all DON CMS accounts per references (i) and (ab).

REFERENCES

(a) Executive Order 12958, *Classified National Security Information*, 17 Apr 95

(b) *Office of Management and Budget, Implementing Directive* for E.O. 12958, 32 CFR Part 2001, 13 Oct 95

(c) *Subpart D, "Safeguarding" of Information Security Oversight Office (ISOO) Directive 1*, 25 Jun 82

(d) DoD Directive 5200.1, *DoD Information Security Program*, 13 Dec 96 (NOTAL)

(e) DoD 5200.1-R, *DoD Information Security Program Regulation*, 14 Jan 97 (NOTAL)

(f) Executive Order 12829, *National Industrial Security Program*, 6 Jan 93

(g) DCID 1/7, *Security Controls on the Dissemination of Intelligence Information*, 30 Jun 98 (NOTAL)

(h) *DOE Final Rule on Nuclear Classification and Declassification*, 10 CFR, Part 1045, 22 Dec 97 (NOTAL)

(i) CMS-1A, *Cryptographic Security Policy and Procedures Manual (U)*, 25 Feb 98 (NOTAL)

(j) DoD 5105.21-M-1, *DoD Sensitive Compartmented Information Administrative Security Manual*, 3 Aug 98 (NOTAL)

(k) DoD Directive 0-5205.7, *Special Access Program (SAP) Policy*, 13 Jan 97 (NOTAL)

(l) DoD Instruction 0-5205.11, *Management, Administration, and Oversight of DoD Special Access Programs (SAPs)*, 1 Jul 97

(m) DoD 5220.22-M, *National Industrial Security Program Operating Manual (NISPOM)*, Jan 95 (NOTAL)

(n) SECNAVINST S5460.3B, *Control of Special Access Programs Within the Department of the Navy*, 30 Aug 91 (NOTAL)

(o) OPNAVINST S5460.4C, *Control of Special Access Programs Within the Department of the Navy* (U), 14 Aug 81 (NOTAL)

(p) OPNAVINST S5511.35K, *Policy for Safeguarding the Single Integrated Operational Plan (SIOP) (U)*, 1 Jul 98 (NOTAL)

(q) NAVSEAINST C5511.32B, *Safeguarding of Naval Nuclear Propulsion Information (NNPI) (U)*, 22 Dec 93 (NOTAL)

(r) Title 42, U.S.C., Sections 2011-2284, *Atomic Energy Act* of 30 Aug 54, as amended

(s) DoD Directive 5210.2, *Access to and Dissemination of Restricted Data*, 12 Jan 78 (NOTAL)

(t) USSAN 1-69, *United States Implementation of NATO Security Procedures*, 21 Apr 82 (NOTAL)

(u) OPNAVINST C5510.101D, *NATO Security Procedures (U)*, 17 Aug 82 (NOTAL)

(v) Title 50, U.S.C., Section 403(g), *National Security Act*

(w) DoD 5200.2-R, *DoD Personnel Security Program Regulation*, 19 Jan 87 (NOTAL)

(x) SECNAVINST 5510.30A, *DON Personnel Security Program Regulation*, 10 Mar 99

(y) DoD Directive 5200.1-M, Acquisition System Protection *Program*, 16 Mar 94 (NOTAL)

(z) SECNAVINST 5239.3, *Department of the Navy Information Systems Security (INFOSEC) Program*, 14 Jul 95 (NOTAL)

(aa) OPNAVINST 5239.1A, *Department of the Navy Automatic Data Processing Security Program*, 3 Aug 82

(ab) CMS-21 Series, *Interim CMS Policy and Procedures for Navy Tier 2 Electronic Key Management System*, 30 May 97 (NOTAL)